



3/25/2021

Hands On Exercise

Chapter 5

Managing Group Policies

(Part1)

El Adel, Taoufik

IT 416 - SPRING 2021 - OLD DOMINION UNIVERSITY

Table 5-1 Activity requirements

Activity	Requirements	Notes
Activity 5-1: Resetting Your Virtual Environment	ServerDC1, ServerDM1	
Activity 5-2 Working with GPO Inheritance Blocking and Enforcement	ServerDC1, ServerDM1	
Activity 5-3: Using GPO Security Filtering	ServerDC1, ServerDM1	
Activity 5-4: Using GPO Security Filtering for a Computer Account	ServerDC1, ServerDM1	
Activity 5-5: Configuring Loopback Policy Processing	ServerDC1, ServerDM1	
Activity 5-6: Using Remote Group Policy Updates	ServerDC1, ServerDM1	
Activity 5-7: Using Group Policy Results and Group Policy Modeling	ServerDC1, ServerDM1	
Activity 5-8: Backing Up and Restoring a GPO	ServerDC1	

Activity 5-1: Resetting Your Virtual Environment

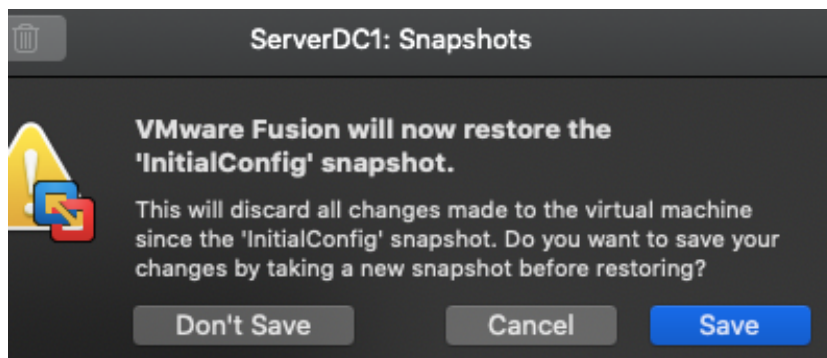
Time Required: 5 minutes

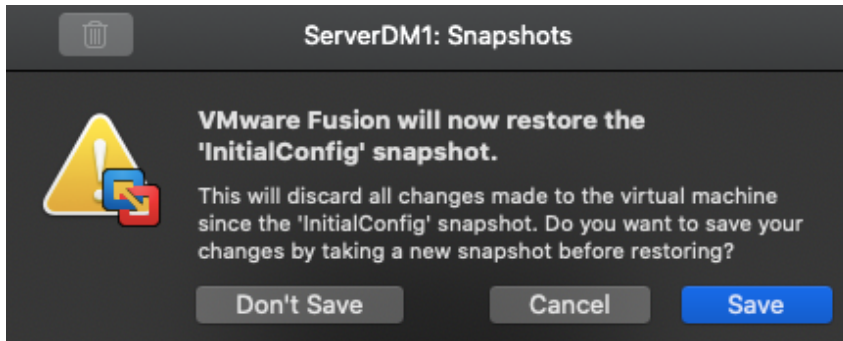
Objective: Reset your virtual environment by applying the InitialConfig checkpoint or snapshot.

Required Tools and Equipment: ServerDC1, ServerDM1

Description: Apply the InitialConfig checkpoint or snapshot to ServerDC1 and ServerDM1.

1. Be sure the servers are shut down. In your virtualization program, apply the InitialConfig checkpoint or snapshot to ServerDC1 and ServerDM1.
2. When the snapshot or checkpoint has finished being applied, continue to the next activity.





Activity 5-2: Working with GPO Inheritance Blocking and Enforcement

Time Required: 20 minutes

Objective: Use the Block Inheritance option on an OU and the Enforcement option on a GPO.

Required Tools and Equipment: ServerDC1, ServerDM1

Description: In this activity, you configure a policy to prohibit access to Control Panel. Then you block inheritance to see that the policy doesn't affect objects below where inheritance blocking is enabled. Then, you configure the enforcement option on the GPO to see that GPO enforcement option overrides the block inheritance option.

1. Sign in to ServerDC1 as **Administrator**, and open the Group Policy Management console.
2. Create a GPO named **GPO1** in the Group Policy Objects folder. Open GPO1 in the Group Policy Management Editor (GPME).
3. Navigate to **User Configuration\Policies\Administrative Templates\Control Panel**. In the right pane, double-click the **Prohibit access to Control Panel and PC settings** policy. Click **Enabled** to enable the policy. Read the Help information so that you know what the policy does. Click **OK**. Close GPME.
4. Link GPO1 to the domain by right-clicking **MCSA2016.local** and clicking **Link an Existing GPO**. Click **GPO1** and click **OK**.
5. Open Active Directory Users and Computers. Right-click **MCSA2016.local**, point to **New**, and click **Organizational Unit**. Type **TestOU1** and click **OK**.
6. Click the **Users** folder and then drag and drop **domuser1** to **TestOU1**. Click **Yes** to confirm. Close Active Directory Users and Computers.

- On ServerDM1, sign in as **domuser1**. Right-click **Start** and click **Control Panel**. You should see a message that the operation has been canceled due to restrictions (see Figure 5-9). Click **OK**. As you can see, domuser1 is restricted from using Control Panel. Sign out of ServerDM1.



Figure 5-9 The message indicating the Control Panel is restricted

- On ServerDC1, in Group Policy Management, right-click **TestOU1** and click **Block Inheritance**. You see a blue circle with a white exclamation point indicating that inheritance is blocked. Now users in TestOU1 aren't affected by GPOs linked to the domain.
- On ServerDM1, sign in again as **domuser1**. Right-click **Start** and click **Control Panel**. Control Panel opens normally because the policy setting in GPO1 is being blocked. Sign out of ServerDM1.
- On ServerDC1 in Group Policy Management, right-click **GPO1** under the domain node and click **Enforced**.
- Sign in to ServerDM1 as **domuser1**. Right-click **Start** and click **Control Panel**. You should see the message that the operation has been canceled due to restrictions. Click **OK**. As you can see, domuser1 is once again restricted from using the Control Panel because enforcement overrides block inheritance. Sign out of ServerDM1.
- On ServerDC1, right-click **GPO1** under the domain node and click to uncheck **Enforced**. Right-click **TestOU1** and click to uncheck **Block Inheritance**.
- Continue to the next activity.

GPO1 [SERVERDC1.MCSA2016.LOCAL] Policy	Setting	State
Computer Configuration	Add or Remove Programs	
> Policies	Display	
> Preferences	Personalization	
User Configuration	Printers	
> Policies	Programs	
> Software Settings	Regional and Language Options	
> Windows Settings	Hide specified Control Panel items	Not configured
> Administrative Templates: Policy c	Always open All Control Panel Items when opening Control ...	Not configured
> Control Panel	Prohibit access to Control Panel and PC settings	Enabled
> Desktop	Show only specified Control Panel items	Not configured
> Network		
> Shared Folders		

MCSA2016.local

Status	Linked Group Policy Objects	Group Policy Inheritance	Delegation		
	Link Order	GPO	Enforced	Link Enabled	GPO Status
	1	Default Domain Policy	No	Yes	Enabled
	2	GPO1	No	Yes	Enabled

Active Directory Users and Computers

File Action View Help

The screenshot shows the Active Directory Users and Computers console. The left pane displays a tree view with the following structure:

- Active Directory Users and Computers
- Saved Queries
- MCSA2016.local
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Managed Service Accounts
 - Users
 - TestOU1 (selected)

The right pane shows a list of users with the following columns:

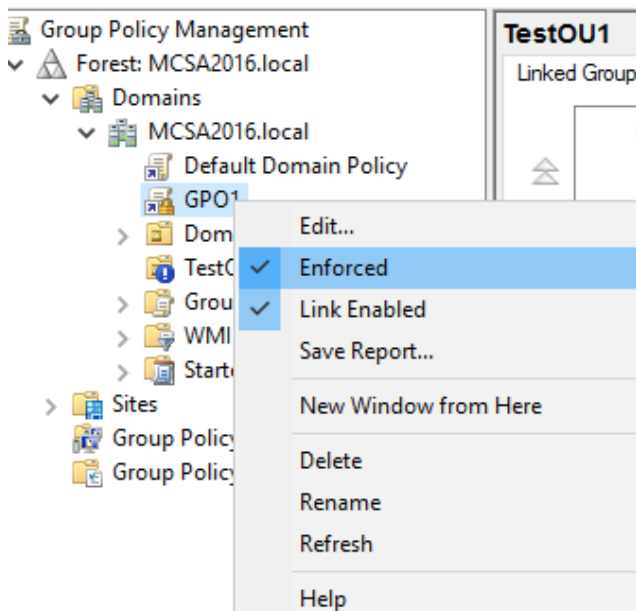
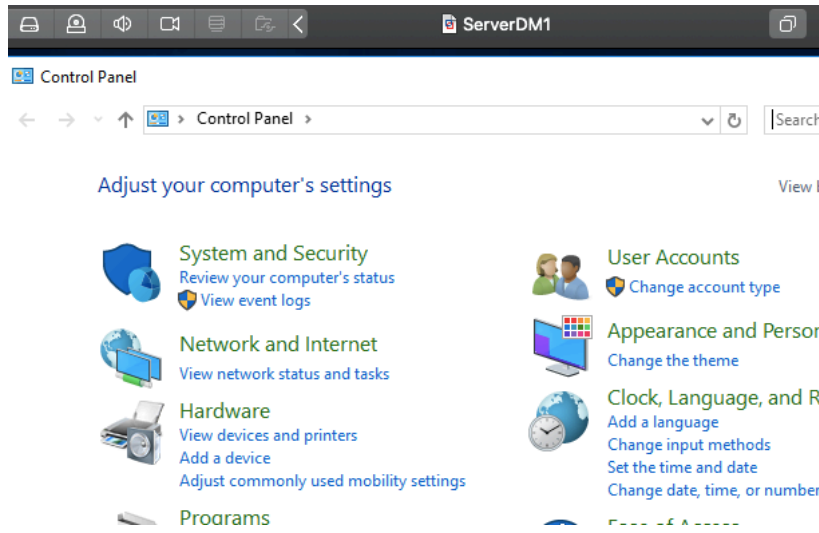
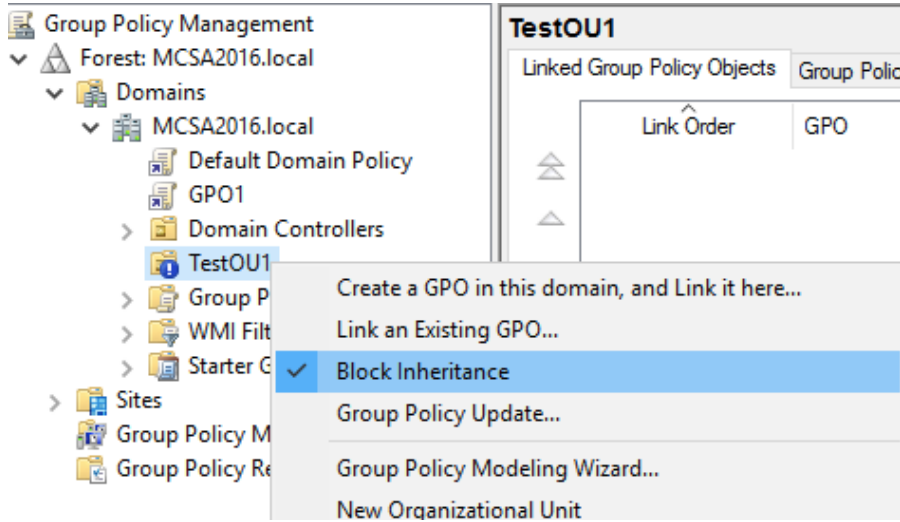
Name	Type
domuser1	User

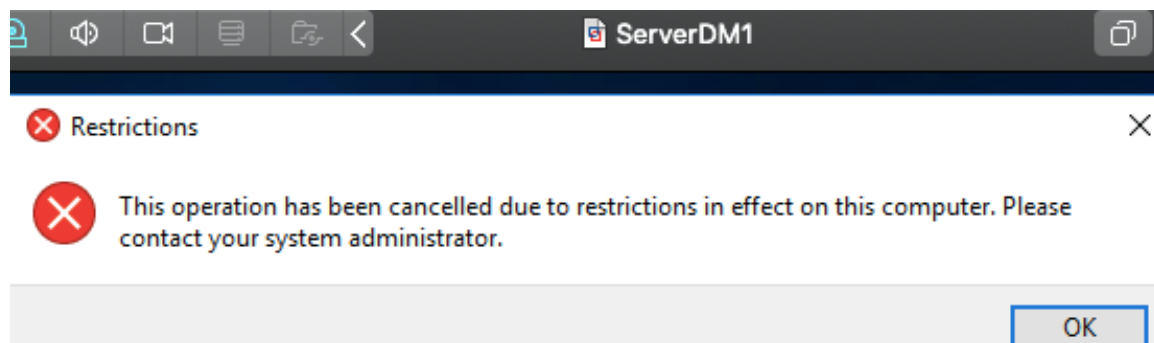
The screenshot shows a Windows error dialog box titled "Restrictions" with the following text:

Restrictions

This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

OK





Activity 5-3: Using GPO Security Filtering

Time Required: 15 minutes

Objective: Change the default security filtering on a GPO and examine the results.

Required Tools and Equipment: ServerDC1, ServerDM1

Description: In this activity, you use GPO filtering to change the default inheritance behavior of GPO processing.

1. On ServerDC1, in the Group Policy Management console, click to expand the **Group Policy Objects** folder, and then click **GPO1**. In the right pane, click the **Scope** tab, if necessary.
2. In the Security Filtering dialog box in the right pane, click the **Add** button. Type **domuser2**, click **Check Names**, and then click **OK**.
3. Click the **Delegation** tab. Click **Advanced**. In the top pane of the GPO1 Security Settings dialog box, click **Authenticated Users**. In the bottom pane, scroll down and click to clear **Apply group policy** (see Figure 5-10). Click **OK**.

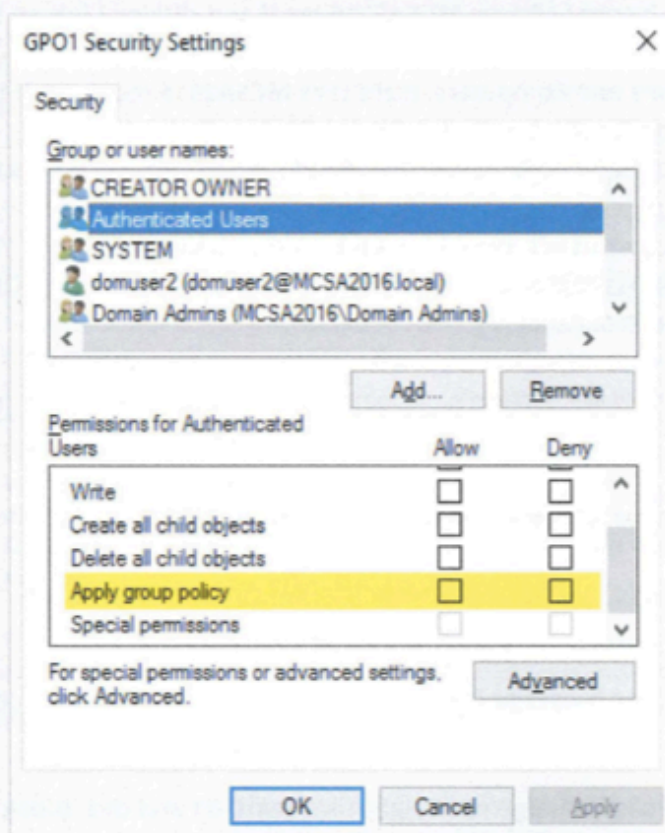


Figure 5-10 Setting GPO security

4. Click the **Scope** tab again. Now domuser2 is the only security principal with Read and Apply Group Policy permissions for GPO1.

Note

Authenticated Users must have the Read permission in order for other users to access a GPO. This is unexpected but a known issue.

5. GPO1 is still linked to the domain object, so there's no need to link it to a container. On ServerDM1, sign in as **domuser1**. Right-click **Start** and click **Control Panel**. Control Panel opens normally because only domuser2 has permission to read the GPO1 Group Policy object that restricts access to Control Panel.
6. Sign off ServerDM1 and sign in as **domuser2**. Right-click **Start** and click **Control Panel**. You should see the message that the operation has been canceled due to restrictions because domuser2 has permission to read the GPO that restricts access to Control Panel. Sign out of ServerDM1.
7. On ServerDC1, click to select **GPO1**, if necessary, and click the **Scope** tab, if necessary. Click **Add**, type **Authenticated Users**, and click **Check Names**. Click **OK**. Click **domuser2**, click **Remove**, and click **OK**.
8. Right-click **GPO1** under the domain node and click **Delete** to unlink it.
9. Continue to the next activity.


GPO1

Scope **Details** Settings Delegation Status

Links



Display links in this location:

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
 MCSA2016.local	No	Yes	MCSA2016.local

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
 Authenticated Users
 domuser2 (domuser2@MCSA2016.local)

GPO1 Security Settings

Security

Group or user names:

- CREATOR OWNER
- Authenticated Users
- SYSTEM
- domuser2 (domuser2@MCSA2016.local)
- Domain Admins (MCSA2016\Domain Admins)

Add... Remove

Permissions for Authenticated Users

	Allow	Deny
Write	<input type="checkbox"/>	<input type="checkbox"/>
Create all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Delete all child objects	<input type="checkbox"/>	<input type="checkbox"/>
Apply group policy	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Special permissions	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

Advanced

GPO1

Scope Details Settings Delegation Status

Links

Display links in this location: MCSA2016.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
MCSA2016.local	No	Yes	MCSA2016.local

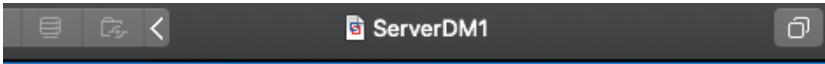
Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
domuser2 (domuser2@MCSA2016.local)

```
C:\Users\domuser1>gpupdate
Updating policy...
```







```
Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

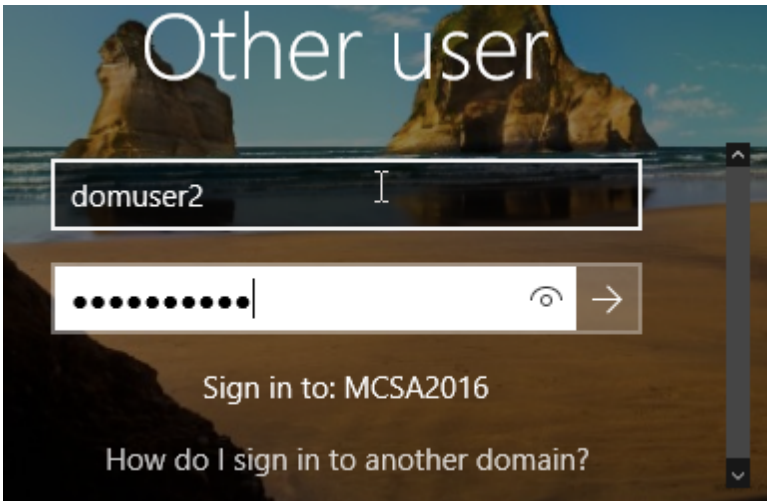


Control Panel

→ > Control Panel >

Adjust your computer's settings

 System and Security Review your computer's status View event logs	 User Accounts Change your user account's appearance
 Network and Internet View network status and tasks	 Appearance Change the look of Windows
 Hardware View devices and printers Add a device	 Clock, Language, Region Add a language Change the time zone Set the time



Restrictions [Close]

This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

OK